

WILTSHIRE FIRE & RESCUE SERVICE

Manor House, Potterne, DEVIZES, Wiltshire, SN10 5PP
Telephone (01380) 731170



Information Management Corporate Code of Conduct For Members, Officers and Staff



Awarded for excellence

CONTENTS Page

INTRODUCTION	1
Definitions of Terms Used within this Document	1
Offences under the Law	2
The Data Protection Act 1998	2
The Freedom of Information Act 2000	2
The Human Rights Act 1998	2
The Crime and Disorder Act 1998	2
The Computer Misuse Act 1990	2
Advice, Information and Support	2
Principles of the Data Protection Act 1998	2
Scope and Coverage of the Data Protection Act 1998	3
Scope and Coverage of the Freedom of Information Act 2000	4
Wiltshire Fire & Rescue Service Management Structure	4
The Management Board	4
The Data Protection Officer	5
The Information/Data Security Officer	5
The Department Heads/Information Managers	6
All Other Persons Employed by the Service	6
Persons Undertaking Work for, or on Behalf of the Service	6
Reference to Schedules 2 and 3 of the Data Protection Act 1998	6
Employee/Employer Relationships	8
Staff 'Fair Capture' Statement	8
Relationships with the Public	9
Public 'Fair Capture' Statement	9
Formal Requests for Access to Personal Data	10
Requests for Information Under the Freedom of Information Act	10
Re-Use of Public Sector Information	12
Comments, Complaints, and Appeals	15

APPENDICES

I Storage of Personal Data – Retention Times

Bases for Recommendations

Recommendations – A General

B Finance and Accountancy

C Human Resources/Personnel

D Medical Records and Health and Safety at Work.

INFORMATION MANAGEMENT CODE OF CONDUCT FOR MEMBERS, OFFICERS AND STAFF INTRODUCTION

1. The Management Board of the Wiltshire Fire & Rescue Service are fully committed to assuring the privacy, security and continuing availability of our corporate information resources. This ensures our compliance with all extant legislation in relation to, the capture, storage, processing, disclosure and disposal of that information.
2. What follows is our Code of Practice defined to support the documented Corporate Policy in Regard to Compliance with the Data Protection Act 1998, the Corporate Policy with Regard to Compliance with the Freedom of Information Act 2000 and the Re-Use of Public Sector Information Regulations 2005, associated procedures and practices adopted by the Wiltshire Fire & Rescue Service.
3. The Code also outlines the relevant issues raised by other existing legislation including:
 - a. The Human Rights Act 1998.
 - b. The Crime and Disorder Act 1998.
 - c. The Computer Misuse Act 1990.
4. Compliance with this Code of Conduct shall be mandatory for all Members of the Wiltshire Fire & Rescue Service, for all officers and full or part time staff directly employed by the Service and for all persons engaged to undertake, in any capacity, work for or on behalf of the Service.

DEFINITIONS OF TERMS USED WITHIN THIS DOCUMENT

6. Terms used within this document are defined within the Data Protection Act 1998 and include:
 - a. **Personal Data** – Data from which a living individual, or living individuals, may be identified.
 - b. **Data Subject(s)** – The person(s) to whom the information refers.
 - c. **Data Controller** – The organisation capturing, storing and processing Personal Data.
 - d. **Data Processor** – Any person or organisation processing the data for, or on behalf of, the Data Controller.
 - e. **Record** – Any structured information stored, on paper (hard copy), magnetic media or otherwise electronically, for processing whether by manual or automated system.

OFFENCES UNDER THE LAW

7. The Data Protection Act 1998 introduces a number of offences in relation to the Data Controllers' failure to submit a formal Notification to the Information Commissioner and to non-compliance with the eight Principles of the Act. (Paragraph 6 refers). This Code specifically addresses the Service's responsibilities to protect the rights and freedoms of the individual as provided for in Part II of the Act, 'The Rights of Data Subjects and Others'.

8. The Freedom of Information Act 2000 encourages greater openness and accountability in government by requiring that anyone making a request for information to a Public Service is entitled to be informed in writing whether or not it holds information of the nature requests and, if that is the case, to have that information communicated to them. (Paragraph 20, post, refers) The Act also, to some extent, modifies the Data Protection Act 1998. It is a specific offence under the Act to alter records in order to avoid disclosure.

9. The Human Rights Act 1998 provides everyone within the United Kingdom to the rights and freedoms of the individual under the European Convention on Human Rights. The Act (Section 6) states that 'it is unlawful for any Public Service to act in any way which is incompatible with a Convention Right'. The Act goes on to redefine 'to act' to include 'to fail to act'. It also provides that a person who, claiming that a public Service has acted or proposes to act in a way which is made unlawful by the Act, and being a victim of that unlawful act, may bring proceedings against the Service in an appropriate court or tribunal

10. The Crime and Disorder Act 1998 enables public bodies working together to reduce the risks, or effect prosecution, of crime and disorder offences. This co-operation is effected by the exchange of information (data sharing), particularly between the 'emergency services', and represents a high risk of failure to comply with one or more the three preceding acts. This is particularly relevant to Service staff that record incidents on video or photographs, or a fire report, which may be requested by the police for evidence in a prosecution. When addressing crime and disorder matters, Members, Officers and staff of the Service must at all times be aware of the constraints imposed by these other Acts and seek to justify any disclosures made by reference to the legal exemptions.

11. The Computer Misuse Act 1990 introduced three offences relating to the deliberate misuse of computer systems; they address unauthorised access, unauthorised modification of records and ulterior intent. There is no specific body established to monitor national compliance with the Act. The police and the courts deal with offences.

12. The fundamental rights and freedoms assigned the individual under the above Acts are subject to exemptions based upon the public interest. Interpretation of the provisions will often be difficult and it is recommended that Members, officers and staff of the Service think carefully about the justification for their act, or failure to act, before proceeding. Advice, information and support are made available through the Clerk to the Service, Data Protection Officer and/or the Information/Data Security Officer

THE PRINCIPLES OF THE DATA PROTECTION ACT 1998

13. The Act, together with its secondary legislation, which implements the European Data Protection Directive in the United Kingdom, received the Royal Assent in July 1998 and came into force on March 1st 2000.

14. The Act fully replaces the Data Protection Act 1984 and establishes eight Principles, the aim of which is to safeguard the privacy of the living individual, these are:

- a. Personal Data shall be processed fairly and lawfully.
- b. Personal Data shall be obtained for one or more specified purposes and shall not be further processed in any manner incompatible with that purpose.
- c. Personal Data shall be adequate, relevant and sufficient but not excessive in relation to the prescribed purpose(s).
- d. Personal Data shall be accurate and where necessary kept up to date.
- e. Personal Data shall be kept for no longer than is essential to the specified purpose(s).
- f. Personal Data shall be processed in accordance with the rights and freedoms of Data Subjects under this Act.
- g. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing and against accidental loss or destruction of the data held.
- h. Personal Data shall not be transferred to a country or territory outside of the European Economic Community unless there is an adequate level of protection for the rights and freedoms of Data Subjects in that country or territory.

SCOPE AND COVERAGE OF THE DATA PROTECTION ACT 1998

15. There are a number of important differences between the Data Protection Act 1984 and the new legislation. However, the new Act still gives certain rights to living individuals in respect of Personal Data held about them by others. Except where it is possible to claim exemption under other provisions of the Act, these Principles apply to all Data Controllers.

16. While the Act of 1998 has retained eight Principles they are not exactly similar to those of the earlier Act.

17. The earlier Act applied only to Personal Data held on automated systems (computers); the new Act effects the inclusion of manually recorded Personal Data and they're relevant filing systems. For the purposes of the Act a 'relevant filing system' is defined as:

“ Any set of information relating to (living) individuals to the extent that, although the information is not processed by means of equipment operating automatically in response to instructions given for that purpose, the set is structured, either by reference to (living) individuals or by reference to criteria relating to (living) individuals, in such a way that specific information relating to a particular (living) individual is readily accessible”

18. It will not always be clear how the foregoing definition should be interpreted. Where doubt exists guidance may be obtained through the inquiry service operated by the Information Commissioner; in extreme cases, disputes will have to be settled by the Courts.

19. The coverage of the Acts does, however, quite clearly include:

- Computer records.
- Video/audio recordings
- Electronic mail systems.
- Structured and unstructured paper files including card indexing systems

SCOPE AND COVERAGE OF THE FREEDOM OF INFORMATION ACT 2000

20. The Freedom of Information Act 2000 makes 'provision for the disclosure of information held by public authorities or by persons providing services for them and to amend the Data Protection Act 1998 and the Public Records Act 1958; and connected purposes'

21. The Act specifically provides that 'any person making a request for information to a public authority is entitled to be informed in writing by the public authority whether it holds information of the nature specified in the request and if that is the case to have that information communicated to him'

22. The duty of the public authority to comply is referred to in the Act as the 'duty to confirm or deny'

23. The Act does, however, provide that information which is reasonably accessible to the applicant otherwise than through a request to the public authority is exempt from the duty to confirm or deny and that:

- a. Information may be 'reasonably accessible' to the applicant.
- b. Information is reasonably available to the applicant if the public authority, or other person, is obliged by law to communicate to members of the public on request.

24. Under Section 19 of the Act the public authority must adopt and maintain a scheme, which relates to the publication of information by the Service and is approved by the Information Commissioner.

25. The public right to information held by a public authority is not, however, absolute. The Act provides that the duty to confirm or deny does not arise in relation to any information in respect of which the Act confers an absolute exemption or in circumstances where the public interest is better served by maintaining the exclusion of the information from disclosure.

26. It is recommended that the management structure established for assuring compliance with the Data Protection Act 1998 also serves to manage corporate compliance with the Freedom of Information Act 2000.

27. The Act covers all information held by the public authority on the media described at paragraph 19 above and applicants are not obliged to identify the Act under which the application is made. This places the Service at risk of failure to comply with the requirements of the Data Protection Act 1998 unless adequate controls are implemented to specifically protect Personal Data.

THE WILTSHIRE FIRE & RESCUE SERVICE MANAGEMENT STRUCTURE

28. Overall responsibility for corporate compliance with the Act shall reside with the Management Board and 'Information Management' shall represent a regularly recurring item on the agenda for the group meetings.

29. Specific responsibility for monitoring corporate compliance with the Act shall be assigned to the Data Protection Officer (The Deputy Chief Fire Officer) who will initiate appropriate checks and report to the Management Board on an exception basis or as and when required by the Chief Fire Officer.

a. To assist him in his duties the Data Protection Officer (DPO) will delegate responsibility for day-to-day corporate compliance with the Act to the Information Rights Advisor.

30. The Information Rights Advisor shall have responsibility for:

a. Provision of advice, information, support and training to all officers and staff of the Wiltshire Fire & Rescue Service on matters concerning information management in general and data privacy and security in particular.

b. Maintenance, up to date, of the Notification of Systems, both automatic and structured manual, submitted to the Information Commissioner in accordance with the requirements of the Act.

c. Definition, documentation and implementation of procedures to ensure prompt and full response to Data Subjects' requests for access to Personal Data; ensuring that action in respect of requests is completed within forty days of receipt of the request and that any subsequent action to be taken is effected within twenty-one days of the requirement being notified by the Data Subject. Procedures should also ensure that any charge levied in respect of the response to a Data Subject Request for Access does not exceed the maximum prescribed in the Act.

d. To define, document and appropriately disseminate a 'publication scheme' for the Service, identifying information already made available to the public through other sources, and describing the procedures for responding to requests for information from members of the public.

e. Definition, documentation and implementation of procedures for prompt and full responses, in accordance with the provisions of the Act, to requests for information, from members of the public.

f. Monitoring, day to day, the Service's compliance with the Principles of the Data Protection Act 1998, the Freedom of Information Act 2000 and with corporate Policy, Codes of Practice, procedures and generally accepted best/ethical practices in relation to the Acts.

g. Providing the essential liaison with the Information Commissioner and sharing, with the DPO, the role of 'central contact' for persons seeking access

to Personal Data, or information under the Freedom of Information Act or persons making inquiries about the practices and procedures adopted by the Service for assuring the privacy, security and continuing availability of information held.

h. Maintaining up to date the knowledge and skills relevant to the effective discharge of his duties.

i. Advising the Monitoring Officer of any changes in Policy or amendments.

31. All Department Heads and some additional, clearly assigned, officers will assume the responsibilities associated with the day to day management of the Service's information resources. These 'Information Managers' will, primarily, define, document and disseminate procedures to ensure that the information used within their department/specialist area is;

a. Captured fairly and lawfully;

b. For a specified purpose or purpose(s);

c. Relevant, adequate but not excessive in respect of that purpose or purposes;

d. Kept up to date where necessary;

e. Securely disposed of when no longer required for the specified purpose(s);

f. Secured against accidental or malicious alteration or deletion and against unauthorised disclosure.

ALL OTHER PERSONS DIRECTLY EMPLOYED BY, AND THOSE UNDERTAKING WORK FOR AND ON BEHALF OF, THE SERVICE

32. The Act imposes upon the Service the responsibility to ensure that all permanent and part time members of staff and any individual or organisation undertaking work for or on behalf of the Service are aware of their individual responsibilities under the Act.

33. All members of the Service's staff have a personal responsibility to safeguard Personal Data against unauthorised disclosure, alteration or deletion.

34. Contractors and other individuals or organisations undertaking work for or on behalf of the Service must be contractually obliged to comply with the standards for data privacy, security and continuing availability adopted by the Service.

REFERENCE TO SCHEDULES 2 AND 3 OF THE DATA PROTECTION ACT 1998

35. In order to satisfy the requirement to capture Personal Data fairly and lawfully reference shall be made to Schedule 2 of the Data Protection Act 1998. This schedule provides that data is captured fairly if:

- a. The Data Subject has given consent.
- b. The processing is necessary for the performance of a contract to which the Data Subject is a party or the taking of steps, at the request of the Data Subject, with a view to entering into a contract.
- c. The processing is necessary to comply with any legal obligation to which the Data Controller is subject.
- d. The processing is necessary in order to protect the vital interests of the Data Subject.

In order to satisfy the requirement to capture sensitive¹ Personal Data fairly and lawfully reference shall be made to Schedule 3 of the Data Protection Act 1998. The Third Schedule provides that data is fairly captured if:

- a. The Data Subject has given explicit consent to the processing.
- b. The processing is necessary for the purposes of exercising or performing any right or obligation that is conferred or imposed by Law in connection with employment.
- c. The processing is necessary in order to protect the vital interests of the Data Subject or another in a case where consent cannot be given by, or on behalf of the Data Subject:
 - i. The Data Controller cannot reasonably be expected to obtain the consent of the Data Subject.
 - ii. In order to protect the vital interests of another person in a case where the consent of the Data Subject has been unreasonably withheld.
- d. The processing:
 - i. Is carried out in the course of legitimate activities of political, religious, body or association not established for profit.
 - ii. Is carried out with appropriate safeguards for the rights and freedoms of the Data Subject.
 - iii. Relates only to members of the body or association.
 - iv. Does not involve disclosure of data to a third party without the consent of the Data Subject.
- e. The Personal Data has been made public as a result of steps deliberately taken by the Data Subject.

¹

Sensitive Data: Data which refers to the racial origin, political opinions, religious beliefs, physical or mental health, sexual life, commission or alleged commission of an offence or the proceedings for any offence committed, the disposal of such proceedings and/or the sentence of the court in such proceedings (Section 2 DPA 1998)

- f. The processing is necessary for the:
 - i. Purposes of, or in connection with, any legal proceedings.
 - ii. Purpose of obtaining legal advice.
 - iii. Purposes of establishing, exercising or defending legal rights.
- g. The processing is necessary for the:
 - i. Administration of justice.
 - ii. Exercise of any functions conferred under any enactment.
 - iii. Exercise of any functions of the Crown, a Minister of the Crown or a Government Department.
- h. The processing is necessary for medical purposes if undertaken by a health professional or a person who holds duty of confidentiality equivalent to a health professional.
 - i. The processing is of a sensitive nature relating to ethnic or racial origin, or:
 - ii. Is necessary for the purpose of identifying existence or absence of racial equality.
 - iii. Is carried out with appropriate safeguards for the rights and freedoms of the Data Subject.

37. Data shall be classified in a manner that facilitates identification of Schedule 2 or Schedule 3 application with specific emphasis upon the recording of the explicit consent of the Data Subject.

EMPLOYEE/EMPLOYER RELATIONSHIPS

38. The Service will necessarily have to capture and process Personal Data in respect of all employees and, to effect compliance with Para 36 above, staff shall be advised of the nature and the purpose of all information held about them and to whom, if anyone, the information of a personal nature will be disclosed.

39. Where practicable and possible forms for the capture of Personal Data shall include a statement to the effect that:

‘The Data Protection Act 1998

The personal information that you provide on this form is for the purpose of ----- and will not be processed or disclosed in any way incompatible with that purpose. In accordance with the Principles of the Data Protection Act 1998 the information may only be disclosed to the Data Subject (yourself) or with the express permission of the Data Subject EXCEPT where it is required by other enactment to be disclosed to H. M. Inspectors and Collectors of Taxes or to other Central Government agencies. In

order that we may maintain your Personal Data up to date it is essential that you advise immediately of any changes in personal circumstances.

40. Staff shall be advised of the logic involved in the decision taking where automatic processing of Personal Data for purposes such as performance at work, reliability or conduct represents, or is likely to represent, the sole basis for any management decision-making significantly affecting him/her.

41. The Information Rights Advisor shall define, document and implement adequate and effective standards to reduce the risks of:

- a. Inaccurate and/or incomplete data entry.
- b. Inaccurate and/or incomplete amendment of data.

42. The information Rights Advisor responsible for the capture, storage and processing of Personal Data shall ensure continuing data integrity (accuracy, completeness and currency) by the implementation of:

- a. Regular and frequent checks.
- b. Testing routines following the creation of new records and the modification or deletion of existing records.

43. The Information Rights Advisor shall ensure compliance with the fifth Principle of the Data Protection Act 1998 (Personal Data shall be kept for no longer than is essential to the specified Purpose[s]) by defining, where practicable and possible, retention times for Personal Data records. Details of established retention periods may be found at Appendix I.

44. Employees (Data Subjects) shall, periodically, be advised, and asked to confirm the accuracy of standing data held about them. Information Managers shall:

- a. Prepare a schedule of the scope of the data held.
- b. Prepare and maintain a timetable for the implementation of these periodic checks.

45. Details of new processing systems shall be referred to the Data Protection Officer or to the Information Rights Advisor before the system is implemented.

46. Decisions taken to discontinue processing or to delete any Personal Data sets should be communicated to the Information Rights Advisor in order that the Notification to the Information Commissioner may be amended.

RELATIONS WITH THE PUBLIC

47. Whenever practicable and possible members of the public shall be advised of the nature and use of the Personal Data captured and held about them.

48. Forms used for capturing information, from members of the public, of a personal nature shall include a statement to the effect that:

‘The Data Protection Act 1998

The personal information that you provide on this form is for the purpose of ----- and will not be processed or disclosed in any way incompatible with that purpose. In accordance with the Part II, Section 7 of the Data Protection Act 1998 (Rights of Data Subjects and Others) you have the right to be informed whether information of a personal nature is held about you and, if this is the case, to have a description of the data communicated to you. You have the right to require correction or deletion of any information held about you which is inaccurate, incomplete or out of date.

The Service has the right to make a charge, not exceeding the maximum prescribed in the Act, to cover the cost of data retrieval. For a Request for Access to Personal Data held by the Wiltshire Fire & Rescue Service or for further information in respect the Service’s procedures for information privacy and security contact:

The Information Rights Advisor
Wiltshire Fire & Rescue Service,
The Manor
POTTERNE
Wiltshire
SN10 5PP

49. The Information Manager responsible for the capture, storage and processing of the data shall define, document and implement adequate and effective standards to reduce the risks of:

- a. Inaccurate and/or incomplete data entry.
- b. Inaccurate and/or incomplete amendment of data.

50. The Information Manager responsible for the capture, storage and processing of Personal Data shall ensure continuing data integrity (accuracy, completeness and currency) by the implementation of:

- a. Regular and frequent checks.
- b. Testing routines following the creation of new records and the modification or deletion of existing records.

51. Information Managers shall prepare and maintain a schedule of, and monitor all routine disclosures of Personal Data and refer any requests for disclosure of data to the Data Protection Officer or the Information Rights Advisor.

52. Details of new processing systems shall be referred to the Data Protection Officer or to the Information Rights Advisor before the system is implemented.

53. Decisions taken to discontinue processing or to delete any Personal Data sets shall be communicated to the Information Rights Advisor in order that the Notification to the Information Commissioner may be amended.

FORMAL REQUESTS FOR ACCESS TO PERSONAL DATA

54. Members of the Public, including employees of the Service, shall be required to submit a written Request for Access to Personal Data in accordance with the documented procedures adopted by the Service.

55. The applicant, on provision of sufficient information to satisfy the Service as to his/her identity and to facilitate retrieval of the information requested, shall receive a response within forty days of receipt by the Service of the written request.

56. The applicant, on provision of sufficient evidence of the lack of integrity (accuracy and completeness) of the information held or its lack of currency shall be notified of the correction or deletion of the information within twenty-one days of receipt of the evidence.

REQUESTS FOR INFORMATION UNDER THE FREEDOM OF INFORMATION ACT

57. An applicant must submit the application in writing giving:

- a. Name and address.
- b. A description of the information requested.

58. As the applicant is not obliged to state under which Act the application is made the Information Rights Advisor will confirm whether the request is in respect of Personal Data of which the applicant is the Data Subject. If this is the case the application will be handled in accordance with the procedures for Requests for Access to Personal Data, paragraphs 54 -56 refer.

59. Applications for access in accordance with the provisions of the Freedom of Information Act 2000 will be scrutinised to identify any Personal Data and/or data exempt from disclosure under Section II of the Act

60. Where the decision is taken not to disclose information requested the applicant will be advised of the circumstances leading to the refusal and given the opportunity to appeal against the decision.

61. Fees/Charging/Time Limits for Response:

- a. Before retrieving the information for disclosure each request will be estimated as to its total cost. Requests will be free of charge up to £450.00. The Service has twenty days, after the receipt of the written application or website online form to respond to the applicants' request.
- b. In estimating the total cost of a request, search and collation time will be charged at £25.00 per person per hour. The FOI Act also allows for disbursements to be charged such as reproduction and postage charges. In estimating the total cost the time spent on applying the 'public interest test will not be included.
- c. If this amounts to more than £450.00, the request can be refused.
- d. The applicant must be told of any applicable charges and advised that the information will not be forwarded until the agreed fee is paid.
- e. The Finance Unit should be asked to raise and send an invoice as soon as both parties agree the charge.
- f. Once the detailed request and any applicable fees have been received, the search for information can begin.
- g. The Act gives us 20 working days to provide a response.

WILTSHIRE FIRE & RESCUE SERVICE RE-USE OF PUBLIC SECTOR INFORMATION

INTRODUCTION

62. The Government has passed new legislation governing the re-use of public sector information. These Regulations came into effect on 1 July 2005 and are to encourage the re-use of information held by public authorities. The Re-use of Public Sector Information Regulations provide for third parties to re-use information, which is accessible from public sector bodies, including the Wiltshire Fire & Rescue Service. Information held and stored by the Service has an inherent value, which should be recognised and assessed whether we are prepared to allow others to use it and if appropriate at a cost. This would generate additional funds into the Service. These Regulations take their lead from EU Directive 2003/98/EC on the Re-use of Public Sector Information, which also came into force on 1 July 2005. The Regulations can be viewed at: <http://www.opsi.gov.uk/si/si2005/20051515.htm> and the Directive of the European Parliament can be viewed at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0212:FIN:EN:DOC>

RE-USE OF INFORMATION

63. When the Service releases information which has been requested for example under the terms of the Freedom of Information Act 2000, the applicant or member of the public may request that they re-use the information for commercial purposes. If this was carried out without permission there is a risk that a breach of the Authorities copyright may occur. It is for situations that fall under this category that these regulations are concerned. An example of this would include documents or the statistics recorded into our Fire Service Emergency Cover Model that are requested then reproduced by the applicant into their own work and adopted as their own. A guide to the regulations and best practice is available to view at: <http://www.opsi.gov.uk/advice/psi-regulations/advice-and-guidance/guide-to-psi-regulations-and-best-practice.doc>

SCOPE OF REGULATIONS

64. The re-use of public sector information regulations only apply to us as the Wiltshire Fire & Rescue Service.

TYPES OF INFORMATION AVAILABLE FOR RE-USE

65. This includes:

- Codes of Practice
- Health and Safety guidance
- Leaflets and forms
- Official records of proceedings
- Statistics

APPLYING TO RE-USE INFORMATION

66. To apply to the Service for the re-use of information must be done in accordance with the regulations. In these circumstances the Regulations place on us the following obligations:

- A request must be made in writing, email or utilising the online application form at <http://www.wiltshire.gov.uk/>
- The applicant must state their name
- Give an address, can be email for correspondence
- Specify the document or information requested
- State the purposes for which the document is to be re-used
- Information for re-use must be made available electronically where possible
- There will be no discrimination between applicants making requests for re-use

Conditions for re-use must be made available to the public along with any standard use conditions. The request should then be sent to:

Information Rights Advisor
Wiltshire Fire & Rescue Service
Manor House
Potterne
Devizes
Wiltshire SN10 5PP

Or by email to:

mailto: emma.roberts@wiltshire.gov.uk

67. A reply must be sent within 20 working days (beginning from the first working day after the request is received) for a response to a request for re-use. This period may be extended where the request is extensive or complex. In this case, communication about the delay with the applicant becomes important.

Some information will be re-useable free of charge although a licence fee can be issued in certain circumstances. Each response will detail any conditions for re-use.

COPYRIGHT

68. The supply of documents or information to a member of the public by the Service under the Freedom of Information Act does not give them the right to re-use the information in a way that would infringe that copyright. For example by making photocopies, publishing and issuing copies to the public or to any other person. Brief extracts of any of the supplied material may be reproduced with our permission under the fair dealing provisions of the Copyright Designs and Patents Act for the purposes of research for non commercial purposes, private study, criticism, reporting, subject to an acknowledgement of ourselves as the copyright owner. Any wider re-use requires our explicit permission. The Service may choose to allow re-use under licence, imposing conditions to the re-use of the information if it is not used in a manner inconsistent with our copyright and we may also decide to levy a charge.

EXEMPTIONS TO RE-USE

69. Once it is agreed to make information available for re-use the basis on which it is specifically provided will be limited.

Re-use can be refused if:

- The activity of supplying the information or document is one which falls outside our public tasks
- The information or document contains content in which relevant intellectual property rights are owned by a third party
- The content of the information or document is exempt from access by virtue of the freedom of Information Act 2000.

CHARGES

70. The Regulations allow for public authorities to earn a return on their investment by making a reasonable charge on the re-use of information or documents.

In calculating a licence fee the Service will take into account the following

- The Service's intellectual property rights in information that has a commercial value

A charge for this would be determined on a case-by-case basis.

- Charges for staff time

Hourly charges in respect of staff time in making the requested information available to an applicant for re-use will be made in accordance with one of the following rates (these may be subject to revision) depending on the seniority of the member of staff who is required to manage the request.

- £25 per hour, £50 per hour, £100 per hour, or £125 per hour.

Charges for materials:

- Photocopying & printing out (black & white) 10p per sheet any size
- Photocopying & printing out (Colour) 60p per sheet any size
- CD & DVD disks £2 per disk

INFORMATION ASSET LIST

71. Where permission for re-use is granted, a list of the type of information that has received permission for re-use must be published. The list is known as an "Information asset list" and is contained in our Publication Scheme, from which other relevant information can be obtained.

COMPLAINTS

72. A member of the public /the applicant may complain about how the Service has managed their request for re-use e.g. The licence fee they have been charged for the re-use of information.

The complaints procedure set up by the Regulations is to follow the same process as the complaints procedure given under the Freedom of Information Act 2000. However, the Office of Public Sector Information (OPSI) not the Information Commissioner is the ultimate authority. Complaints to OPSI will only be received

after an appeal has been made to the Service and the applicant is not satisfied with the response.

The Act establishes a 2-stage appeal process. Firstly it is required that the applicant makes an appeal to the Service within 4 weeks from receipt of the original decision. This will then be dealt with under the terms of the Service's internal complaints procedure. The Service has then 3 weeks to address the complaint and reach a decision. In this instance complaints are to be directed to:

Wiltshire Fire & Rescue Service Administrative Officer
Manor House
Potterne
Devizes
Wiltshire SN10 5PP

mailto: anna.villette@wiltsfire.gov.uk

Or telephone 01380 731181

If, after the first stage the matter remains unresolved then the complainant is to be directed to the OPSI who are an impartial arbiter. OPSI will only consider a complaint after the former procedures have been exhausted.

All complaints to OPSI must be:

- In writing
- State the nature of the complaint
- Include a copy of the written notification from the Service that outlines our response to the complainant
- Be submitted to OPSI before the end of 28 working days beginning with the date of receipt by them of the Authorities response

The contact details for OPSI are:

The Standards Division
Admiralty Arch
North Side
The Mall
London SW1A 2WH

COMMENTS, COMPLAINTS AND APPEALS DATA PROTECTION & FREEDOM OF INFORMATION ACTS

73. The applicant will be invited to comment on the quality of the service provided by the Information Rights Advisor in respect of any Request for Access to Personal Data.

74. If dissatisfied with the response to a Request for Access to Personal Data, or with decisions taken in regard to a request, the applicant will be advised to, in the first instance, address any comments, complaints and/or appeal to the Service Administrative Officer or the Clerk to the Service if the complaint is in relation to members of the Service.

75. Should the applicant remain dissatisfied, then officers of the Wiltshire Fire & Rescue Service will direct the applicant to address an appeal to the Information Commissioner and afford the applicant every assistance.

**STORAGE OF PERSONAL DATA/ RETENTION TIMES
BASES FOR THE RECOMMENDATIONS.**

1. The recommendations for the retention of Personal Data records which follow have their foundations in existing standards adopted in Public Sector, Corporate Services, Finance and Accounting, Human Resources and Personnel, Training and Staff Development and Legal Services.
2. The standards include known legal requirements, recommendations made by the Audit Commission for Local Authorities [etc] in England and Wales, the relevant professional bodies, and generally accepted best/ethical practices.

RECOMMENDATIONS

A. GENERAL

3. For the purposes of this document the terms 'record(s)' includes Personal Data contained in manual (paper) files, on magnetic media and that stored and processed electronically.
4. The assigned Information Managers should assume responsibility for the documentation, dissemination, implementation and maintenance of the standards in regard to activities falling within their span of control
5. Information Managers must also define procedures for the secure disposal of the Personal Data at the end of the retention period.
6. Personal Data should be further classified as:
 - a. Standing data - that which never or infrequently changes, (e.g. names, addresses, details of next of kin)
 - b. Dynamic data - that which is modified and/or updated on a regular basis (e.g. medical records, performance assessments, conduct reports)
7. It is generally accepted best practice to retain dynamic data as a discrete sub-set of the personnel record files to facilitate review and disposal at the appropriate times. Where practicable and possible annual sub-sets should be maintained so that a routine programme for disposal according to the retention standards may be implemented.

B FINANCE AND ACCOUNTANCY

8. Legislation supporting the activities of the Inland Revenue Department and Her Majesty's Customs and Excise requires that most finance and accounting records, which hold Personal Data within the meaning of the Data Protection Act 1998, are retained for seven and six years respectively.
9. Other financial accounting records should be retained for a minimum of the current plus previous year to facilitate the annual review of major accounting systems undertaken by the Internal Auditor and/or the District Auditor's staff.

C. HUMAN RESOURCES AND PERSONNEL

10. In the interests of privacy and security it is recommended that there should be one copy only of the record types listed below, all of which will be retained by the Human Resources/ Personnel Department. Other Information Managers currently holding such records should discuss secure disposal with the Head of Human Resources and if the need exists, arrange appropriate restricted access to the personnel records. e.g. It is acknowledged that the Occupational Health Officer,

APPENDIX 1 ii

Training and Staff Development Manager and Service Control Officer may need access to up to date information in respect of employee's addresses, home telephone numbers and, in the case of the latter, details of next of kin.

11. The Data Controller must be alert to the presence of Sensitive Personal Data as defined in Schedule 3 of the Data Protection Act 1998. Of particular importance are the Equal Opportunities monitoring processes, which cover race, religion and disability. The Information Commissioner expresses the view that while obtaining the explicit consent of the Data Subject will, in the majority of cases, be an integral function of the data capture questionnaire most monitoring may take place without it.

12. The disposal date may, in some cases, be decided at the time the document is created or be conditional upon the performance/conduct of the Data Subject. e.g. disciplinary action requiring review within a specified timescale.

13. The recommended retention periods for Human Relations/Personnel standing and dynamic data are as follows:

Unsuccessful applications for employment.	Current plus previous year only
Police check information supplied by police – unsuccessful applicants	Destroy immediately
Police check information supplied by the - unsuccessful -applicant	Current plus previous year only
Personnel Record Files generally	Six years after termination of employment EXCEPT where Limitation Act 1980 may be seen to apply then twelve years.
Application Forms (on PRF)	Six years after termination of employment
Equal opportunity monitoring forms.	Current plus previous year only
Referee responses and appointment related correspondence	Current year plus previous three.
Police check information on PRF	Six years after termination of employment
Evidence under the Asylum and Immigration Act (Acceptance for employment in the United Kingdom)	Six months after termination of employment
Evidence of successful applicant's professional and other qualifications on PRF	Six months after termination of employment
Health questionnaires on PRF	Six years after termination of employment.

Letters of Acceptance on PRF	Six years after termination of employment.
Contracts and Terms and Conditions of Service	Six years after termination of employment.
Records having regard to the Working Time Regulations	Six years after termination of employment.
Attendance records other than those used for pay and allowances	Current year plus previous three.
Annual Leave records	Current year plus previous six
Sickness absence records	Current year plus previous six
Special Leave records	Current year plus previous six
Statutory Maternity Leave records, calculations, certificates (MAT B1) and other relevant medical records	Current year plus previous three.
Parental Leave records	Five years from date of birth or adoption or Eighteen years if child is awarded disability allowance.
Staff transfer records (TUPE)	Current year plus previous six
Staff regrading records	Six years after termination of employment.
Training and Staff Development records	Six years after termination of employment.
References provided to employees leaving the Service or testimonials provided to employees leaving the Service on PRF	Six years after termination of employment.
Redundancy details, calculations of payments, refunds, Notification to the Department of the Secretary of State	Limitation Act 1980 recommendations suggest retention for twelve years after termination of employment.
Records of events notifiable under the Retirement Benefits Schemes (Information Powers) Regulations 1995	Six full years from the end of the scheme year in which the event occurred
Records of recommendations for retirement due to incapacity, pension accounts and associated documents	Six full years from the date of signing off the accounts/reports
Records of the appointment and termination of persons to Union Stewards/Convenors positions	Current year plus previous five.
Trades Unions Agreements	Ten years after termination of agreement
Register of Officers Interests/Members Interests	2 years after cessation of employment or membership.
Disciplinary records generally	Variable – see paragraph 7 ante
Grievance resolution records	Six years after termination of employment.
Harassment case documentation	Six years after ruling
Records of Tribunal Proceedings	Six years after ruling

D. MEDICAL RECORDS, HEALTH AND SAFETY AT WORK ACT RECORDS

14. While records in respect of an employee's medical condition are classified 'sensitive Personal Data and subject to the controls defined in Schedule 3 of the Data Protection Act 1998 it should not be assumed that the explicit consent of the Data Subject for processing must always be secured. The Act recognises the legitimate need of employers to keep and to use such records and the Information Commissioner expresses the view that an employer acting in a reasonable manner satisfies other sensitive data processing conditions: e.g the 'legal obligation' of an employer in respect of the Health and Safety at Work (etc) Act and the Disability Discrimination Act.

15. Medical records should, however, form a discrete sub-set of the personnel record file to allow for separate storage facilitating privacy, security and retention controls.

16. The recommended retention periods for medical records and those records maintained in accordance with the provisions of the Health and Safety at Work etc Act.

Medical records generally	Six years after termination of service with the Service
Fitness assessments	For period to next assessment until termination of service with the Service.
Noise at work assessments/Audiometry records	For period to next assessment until termination of service with the Service. Some implication that audiometry records should be retained for forty years.
DSE Records and eye tests	For period until next test until termination of service with the Service
Health records maintained under COSHH Regulation 1994	Forty years from date of exposure.
Employee exposures to hazard – COSHH Regulations 1994	Ten years – to forty years if potential for infection exists.
Accident reports and records	Three years from the date of entry.
Records of tests and examinations of control systems and protective equipment under COSHH Regulations 1994	Five years from the date of the test
Assessments under H&S Regulations and records of consultations with safety representatives/committees	Indefinitely